(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03285 A1

(51) International Patent Classification[7]: G06F 17/60, G07F 7/10, H04L 12/14

(21) International Application Number: PCT/NL01/00508

(22) International Filing Date: 5 July 2001 (05.07.2001)

(25) Filing Language: Dutch

(26) Publication Language: English

(30) Priority Data:
1015612 5 July 2000 (05.07.2000) NL

(71) Applicant: JANSEN, Alexander, Theodorus [NL/NL]; Mgr. Nolensstraat 10, NL-5431 WK Cuyk (NL).

(74) Agent: PRINS, A. W.; Vereenigde, Nieuwe Parklaan 97, NL-2587 BN The Hague (NL).

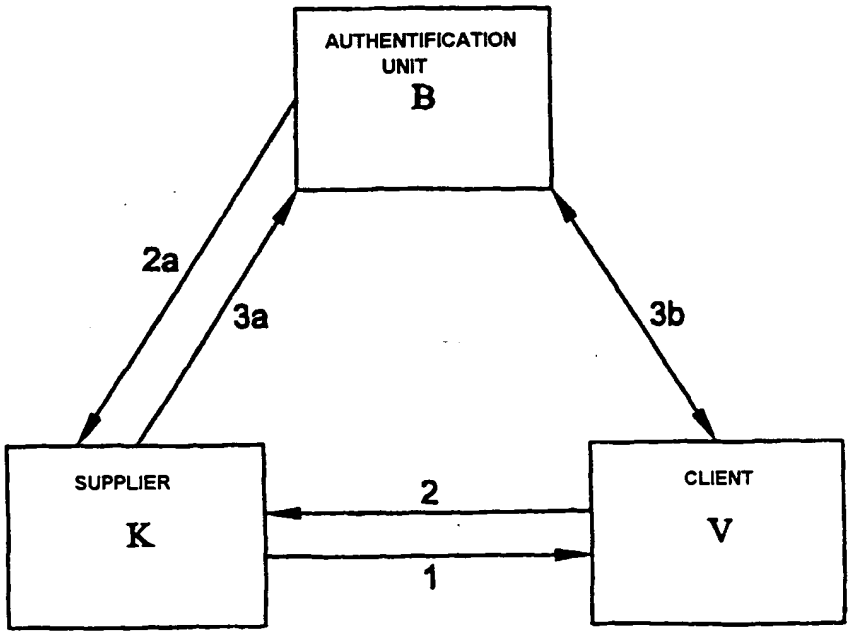
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM AS WELL AS DATA CARRIER FOR AUTHENTICATING A CLIENT WHO DESIRES TO OBTAIN A SERVICE OR PRODUCT FROM A SUPPLIER



(57) Abstract: A method and a system as well as a data carrier for use in a system for authenticating a client who desires to obtain a service or product from a supplier, - wherein the client, via a first communication network, enters into communication with the supplier and gives order information, - wherein the supplier, on the basis of this order information, composes supplier information and gives it to an authentication unit, - wherein the authentication unit, on the basis of the supplier information received, composes authentication information and sends it to the mobile communication network number of the client, - wherein the client, with his mobile communication device, composes reply information and sends it to the authentication unit to confirm the authentication information received., - wherein the authentication unit performs at least one checking step, - wherein, if the or each checking step is followed by a confirmative reply, the authentication unit sends a supply release, - wherein, in a first checking step, the authentication unit checks whether the authentication information sent fits the reply information received.

WO 02/03285 A1

VISAP070.EP 05/09/05
Supplemental Search Report
WO 02/03285 A1

Title: Method and system as well as data carrier for authenticating a client who desires to obtain a service or product from a supplier

This invention relates to a method and a system for authenticating a client who desires to obtain a service or product from a supplier. The invention also relates to a data carrier intended for use in a system according to the invention for carrying out the method according to the invention.

The authentication of a client is particularly important if client and supplier are located at a relatively great distance from each other. The acceptance can take place orally or in writing. The necessary communication means may comprise, for instance, a connection per telephone, fax, telex, telegraph, post or computer network. The offer may have reached the client in different ways, for instance via the above communication means. It is noted that merchandise should be taken widely and may comprise transferable goods as well as services. The services may comprise, for instance, providing access to a computer network, such as an internet, access to specific servers or files on that network, supply of pay television or video-on-demand, or supply of a form of interactive multimedia. The supply of such services can be effected via a telephone or other cable connection, or via a wireless connection of, for instance, a wireless telephone or another wireless communication means.

The connection via a computer network may, for that matter, be established in different ways, for instance by using computer programs already installed on a computer, which programs seek connection with the supplier. Also, the client may make connection with the supplier by using a computer program provided on a computer data storage medium, such as a

CD-ROM or diskette. The computer program may be temporarily entered into the RAM memory of the computer, but the program or associated computer files need not be placed on, for instance, a hard disk of the computer. It should be noted that a CD-ROM may also be a commercially available rectangular CD card, which is intended for use with a CD-ROM player.

A drawback of this method for selling merchandise is that it is difficult, if not impossible, for the supplier to check whether a client is in good or in bad faith. This is increased according as the distance between client and supplier is greater, for instance when client and supplier are in different countries or on different continents. Consequently, this method is relatively susceptible to fraud. A swindler can send, for instance, order information to the supplier, while this person gives incorrect information about his identity. In that case, the person is a pseudoclient. After receipt of the order information, the supplier may proceed to supply, the purchased products or services being put at the disposal of the pseudoclient. After supply, the supplier may try to demand payment from the pseudoclient, which does not succeed if he cannot find out the real identity of the pseudoclient. The same problem may arise if the payment is made by using a credit card number, which, for instance, is usual when selling via a computer network, such as an intranet or internet. A swindler may use a fictitious or a stolen credit card number to mislead a supplier.

It is an object of the present invention to remove the above drawbacks of the method while retaining the advantages thereof. It is therefore an object of the invention to provide a method for selling merchandise that is relatively little susceptible to fraud and gives the supplier more certainty about the identity of the client.

The invention therefore provides a method according to claim 1.

The use of this method provides the supplier with at least two checking means with respect to the identity of the client. The first checking

means is the mobile telephone contact the supplier seeks with the client on the mobile communication network number he has received in the order information. If the order information is correct, he will find that client at that telephone number. If a telephone number is incorrect, this will not be the case. Moreover, the identity of the user of any telephone number can be found out, therefore also the identity of a swindler who calls his own telephone number. This may restrain a swindler from stating his telephone number.

The second checking means is the checking step to be performed by the authentication unit, in which the authentication unit checks whether the authentication information sent fits the reply information received. If the reply information does not have the desired contents, for instance because it does not contain a desired code, the authentication unit will not give a supply release and supply of the product or the service will therefore not take place.

If, during the checking step, the authentication unit discovers a discrepancy, the judgment will be negative. The discrepancy may have arisen because the client is a pseudoclient who has stated a false telephone number in the acceptance, which telephone number is not at his disposal. Consequently, this swindler cannot receive the authentication information. This has the result that the swindler will not be able to send the correct reply information to the authentication unit. Not only the supplier is protected by this method, but also the client is protected against pseudosuppliers. In fact, if a client who is in good faith accepts a purchase agreement and, subsequently, does not receive an authentication information from the authentication unit via his mobile communication network number, he knows or at least can suspect that he has to do with an unreliable supplier. In any case, no purchase can be effected.

According to a further elaboration of the invention, the method is characterized by the measures of claim 2.

Through the addition of the confirmation information to be sent via the first communication network, which information corresponds to the authentication information, and which can therefore only be at the disposal of the client if the authentication information has reached him via his mobile communication number, the supplier is given even more certainty. In fact, on the basis of the confirmation information, the supplier forms double check information and sends it to the authentication unit, which performs a second checking step, the result of which is involved in the sending or not sending of a supply release.

Thus, further checking steps can be added, which increase the security of the method, and which will be described in the subclaims.

The authentication information and the reply information may, for instance, be formed by an SMS message or a communication via the WAP protocol. The reply information may consist, for instance, of a simple reply to the authentication information received. According to a further elaboration of the invention, the authentication information may comprise a description of the products and/or services required by the client, the purchase price, and/or a transaction code.

According to a further elaboration of the invention, the authentication unit forms part of an institution independent of the supplier, such as, for instance, a banking institution or such a checking institution independent of client and supplier. The institution may administer a credit balance of the client, and the institution pays the supplier from the credit balance of the client a purchase price agreed during the supply when the supply release has been sent to the supplier.

Such an independent checking institution, such as, for instance, a banking institution, may function as a reliable third party for the client as well as for the supplier.

Thus, payment can be made rapidly and safely. Moreover, the fact that the client is a client of the checking institution gives the supplier an extra security that the client is reliable.

Preferably, the authentication unit stores the transaction information received from a client or supplier for a limited period of time.

This information is thus prevented from remaining for an unlimited period of time in, for instance, an administrative system of the checking institution through one of the parties, for whatever reason, omitting to send the information required for the supply to the authentication unit.

The supply release can, for instance, give the client an access code, with which access code the client can log into a network server controlled by the supplier, via a network connection of a computer network, so that the client can exchange computer data with this network server. Preferably, the client can only log into the network server of the supplier after the supplier has received a confirmative result from the checking institution about the check or the transaction information from the client received by the checking institution is identical to the received transaction information from the supplier.

This is a reliable method, with which the client can gain access to the information on a server of a computer network controlled by the supplier. The client may, for instance, gain access to computer files, such as sound, picture or video files, which are available on the server after he has logged in. The client may take over these files, for instance by copying them to a computer or mobile telephone controlled by him or to another communication device capable of being coupled to a computer network. Also, the client may use a service delivered to him via the server after logging in. This service may, for instance, comprise participation in a chat box or video conference, or online advice from, for instance, a physician, lawyer, computer expert, broker, notary or patent attorney about matters in which the expertise of the person in question resides.

The invention also provides a system for carrying out the method according to the invention. This system will be described in claim 13.

The automated system comprises computers provided with programs for carrying out this method and peripheral equipment, such as communication means. This is advantageous because such a system can accompany relatively many transactions without using paid workers. Consequently, the method can be carried out relatively rapidly and inexpensively.

The system according to the invention may also assume the form of a vending machine for cigarettes, beverages or medicines. Here the client computer is in the same housing as the supplier computer. In fact, in such a vending machine, the client computer and the supplier computer, and optionally even the authentication computer, may be integrated into the same computer.

The invention further relates to a data carrier, by means of which a computer of a potential client can be made suitable for forming part of the above system as client computer. According to the invention, the data carrier, such as a CD-ROM, a smart card, a floppy disk, or the like, is provided with digital information, which, when entered into the computer of a client, makes this computer suitable as a client computer apparently intended for a system according to the invention. Preferably, the data carrier is a CD-ROM with credit card dimensions, and the information stored thereon is such that, when this information is entered into a computer, this client computer fully automatically leads the client through the purchasing process.

The invention will be described in more detail with reference to three exemplary embodiments and the accompanying drawing.

Fig. 1 shows a schematic diagram of a first exemplary embodiment;

Fig. 2 shows a schematic diagram of a second exemplary embodiment; and

Fig. 3 shows a schematic diagram of a third exemplary embodiment.

In each of Figs. 1-3, a method for authenticating a client who desires to obtain a product or service is schematically shown. A supply agreement is effected through a supplier V receiving an acceptance of an offer or order information from a client K via a communication connection 1. This connection 1 may be, for instance, a telephone connection, or a connection via a computer network, the post, and the like. The acceptance or order information comprises at least one mobile telephone number, and optionally an address for the supply of the merchandise. The order information may likewise comprise a postal code of the client. After receipt of the acceptance, the supplier V or an authentication unit B on behalf of the supplier calls the stated telephone number. Consequently, in the first place, it is found out whether the mobile telephone number is actually used by client K. If the client K has not stated his own telephone number, no telephone connection 2 will be established between the two parties. Consequently, the supplier V knows that the client K is a pseudoclient so that he can prevent himself from being cheated.

If the stated telephone number is correct, the supplier V or the authentication unit B engaged by him will pass authentication information, such as, for instance, a transaction code, to the client K via the connection 2 or 2a. Besides, it can be communicated which merchandise has been purchased, what the agreed purchase price is, and it can be asked whether an optionally stated address of the client K is correct. Subsequently, the client K can give reply information, which, for instance, comprises the transaction code received by him, to the authentication unit B via a mobile communication connection 3a. The authentication unit has already received these data from the supplier in the form of supplier information via connection 3b. Connection 3b may be a normal data network connection. On the basis of the supplier information, the authentication unit has generated the authentication information. Subsequently, the authentication unit B,

which, in this case, is placed with a banking institution, checks whether the reply information fits the authentication information. More in particular, the authentication unit B checks whether the transaction codes received from the client K and supplier V are identical and sends a transaction advice to the supplier, which is dependent on the result of the check. The transaction advice comprises a supply release if the reply information fits the authentication information and does not send such a supply release if the reply information and the authentication information do not fit together. If the result of the check is confirmative, it has been proved that the client K has received his transaction code via his own telephone number and telephone connection 2 or 2a of the supplier V or the authentication unit B engaged by the supplier. This proof is a second guarantee for the supplier V that the client K is in good faith. To carry out this method, the client and the supplier preferably have respectively a client computer KC and a supplier computer VC at their disposal.

In order to build in an additional check, the client, after receipt of the authentication information, which, for instance, comprises a transaction code, can also be requested to send, on the basis of that information, confirmation information to the supplier V. On the basis of this confirmation information, the supplier can compose so-called double check information, which he sends to the authentication unit B via connection 3b. In the authentication unit B, this double check information can be compared with the reply information received. If the double check information fits the reply information, and if also the other checking steps have been completed confirmatively, the authentication unit will send a supply release.

The exemplary embodiment shown in Fig. 2 differs from the exemplary embodiment shown in Fig. 1 in that the supplier information and reply information entering authentication unit B is processed automatically and that payment of a purchase price can be made automatically. To this

end, the banking institution B is provided with an automated information processing system IVS, while the client K has placed a bank balance with the bank. This bank balance is administered by an automated banking system BS. The information processing system IVS is provided with communication means, not shown, so that the client K can send reply information and the supplier V can send supplier information, which, for instance, both comprise a transaction code, to the system IVS via the connections 3a and 3b, respectively. Furthermore, the system IVS is provided with a control, not shown, for instance a computer, which compares the incoming information with each other. The control informs the supplier V of the result of this check. Moreover, the control can pay a purchase price from the bank balance of the client K to the supplier V, which is indicated by an arrow 5. To this end, the control is coupled to the banking system BS via a system coupling 4, which, by order of at least the information processing system IVS, can transfer money from the bank balance to a bank account of the supplier. The coupling 4 between both systems IVS, BS may be, for instance, a computer network connection.

The exemplary embodiment shown in Fig. 3 differs from the exemplary embodiment shown in Fig. 1 in that the supplier V manages a network server S, which communicates with a computer network C. The network server S can supply goods or services to any client K, who therefore has to log into the network server via a network connection 6 by using an access code. To establish this connection 6, the client K can use a computer or mobile telephone connected to the network C or another computer network communication device.

According to the present invention, the client obtains the access code from the supplier V according to the described method for purchasing merchandise. The access code forms part of the transaction information, which the supplier V or the authentication unit B sends to the client K via the telephone connection 2 or 2a. Preferably, the supplier V puts his goods

and/or services to be supplied only at the disposal of the client K if, via communication connection 3b, he has received from the authentication unit B a confirmative result about the check on the transaction information received at the authentication unit B.

It is self-explanatory that the present invention is not limited to the exemplary embodiment described, but that various amendments are possible within the scope of the invention.

CLAIMS

1. A method for authenticating a client who desires to obtain a service or product from a supplier,

- wherein the client, via a first communication network, enters into communication with the supplier,
- wherein the client, via the communication network, gives the supplier order information, which comprises at least one mobile communication network number, at which the client can be reached, and information about the or each service or product the client wishes to obtain,
- wherein the supplier, on the basis of this order information, composes supplier information, which comprises at least the mobile communication network number stated by the client, and gives it to an authentication unit,
- wherein the authentication unit, on the basis of the supplier information received, composes authentication information and sends it to the mobile communication network number of the client via a second mobile communication network,
- wherein the client, with his mobile communication device having the relevant mobile communication network number, composes reply information and sends it to the authentication unit to confirm the authentication information received,
- wherein the authentication unit performs at least one checking step,
- wherein, if the or each checking step is followed by a confirmative reply, the authentication unit sends a supply release to the supplier, on the basis of which the supplier further provides the supply of the service or the product, and wherein, if in one of the at least one checking steps to be performed a negative reply follows, the authentication unit does not send a supply release to the supplier so that supply of the service or the product does not take place,

- wherein, in a first checking step, the authentication unit checks whether the authentication information sent fits the reply information received.

2. A method according to claim 1, wherein the client, after receipt of the authentication information, besides sending via the mobile network of the reply information, also sends to the supplier, via the first communication network, confirmation information corresponding to the authentication information, wherein the supplier, on the basis of the confirmation information, composes double check information and sends it to the authentication unit, and wherein the authentication unit performs a second checking step, in which it is checked whether the double check information fits the reply information.

3. A method according to claim 1 or 2, wherein the supplier information, the authentication information, the reply information and, if applicable, the confirmation information and the double check information all contain a similar transaction code.

4. A method according to any one of claims 1 – 3, characterized in that the authentication unit forms part of an institution independent of the supplier, such as, for instance, a banking institution or such a checking institution independent of the supplier.

5. A method according to claim 4, characterized in that the institution (B) administers a credit balance of the client (K), wherein the institution (B) pays the supplier (V) from the balance of the client (K) a purchase price agreed during the supply when the supply release has been sent to the supplier.

6. A method according to any one of the preceding claims, characterized in that the order information, the supplier information, and the reply information comprise a postal code of the client (K), wherein, in a third checking step, the authentication unit checks whether the postal code of the supplier information corresponds to the postal code of the reply information.

7. A method according to claims 2 and 6, wherein the confirmation information and the double check information also comprise a postal code, wherein, in a fourth checking step, the authentication unit checks whether the postal code stored in the supplier information, the reply information, the confirmation information and the double check information is always the same.

8. A method according to any one of the preceding claims, characterized in that the authentication information comprises a description of the products and/or services required by the client (K).

9. A method according to any one of the preceding claims, characterized in that the authentication information comprises a purchase price of the products and/or services required by the client (K).

10. A method according to any one of the preceding claims, characterized in that the authentication unit (B) stores for a limited period of time the reply information received from a client (K) and/or supplier (V) or supplier information.

11. A method according to any one of the preceding claims, wherein the authentication unit forms part of a system of the supplier.

12. A method according to any one of the preceding claims, wherein the sending of the authentication information and the reply information takes place in the form of a WAP or SMS message.

13. A system for carrying out the method according to any one of the preceding claims, wherein the system comprises a client computer connected to a first communication network, such as, for instance, the internet, a supplier computer connected to a first communication network, and an authentication computer, which is in or can be brought into communication connection with the supplier computer, and which is arranged to send and receive information via a mobile communication network, wherein the client computer is arranged to enter, via the first communication network, into communication with the supplier computer,

- wherein the client computer is arranged to give the supplier computer, via the communication network, order information, which comprises at least one mobile communication network number, at which the client can be reached, and information about the or each service or product the client wishes to obtain,
- wherein the supplier computer is arranged to compose, on the basis of this order information, supplier information, which comprises at least the mobile communication network number stated by the client, and give it to the authentication computer,
- wherein the authentication computer is arranged to compose, on the basis of the supplier information received, authentication information and send it to the mobile communication network number of the client via a second mobile communication network,
- wherein the authentication computer is arranged to receive and process reply information, which reply information has been composed by the client, with his mobile communication device having the relevant mobile communication network number, and sent to confirm the authentication information received,
- wherein the authentication unit is arranged to perform at least one checking step,
- wherein, if the or each checking step is followed by a confirmative reply, the authentication unit is arranged to send a supply release to the supplier computer, on the basis of which the supplier further provides the supply of the service or the product, and wherein, if in one of the at least one checking steps to be performed, a negative reply follows, the authentication unit is arranged not to send a supply release to the supplier so that supply of the service or the product does not take place
- wherein the authentication computer is arranged to check in a first checking step whether the authentication information sent fits the reply information received.

14. A system according to claim 13, wherein the client computer, after receipt of the authentication information, is arranged to send to the supplier computer, via the first communication network, confirmation information corresponding to the authentication information, wherein the supplier computer is arranged to compose, on the basis of the confirmation information, double check information and to send it to the authentication computer, and wherein the authentication computer is arranged to perform a second checking step, in which it is checked whether the double check information fits the reply information.

15. A system according to any one of claims 13 – 14, characterized in that the authentication computer forms part of an institution independent of the supplier, such as, for instance, a banking institution or such a checking institution independent of client and supplier.

16. A system according to claim 15, characterized in that the institution (B) administers a credit balance of the client (K), wherein the authentication computer of the institution (B) is arranged to transfer to the supplier (V) from the bank balance of the client (K) a purchase price agreed during the supply when the supply release has been sent to the supplier.

17. A system according to any one of claims 13 – 16, characterized in that the order information, the supplier information, and the reply information comprise a postal code of the client (K), wherein the authentication unit is arranged to check in a third checking step whether the postal code of the supplier information corresponds to the postal code of the reply information.

18. A system according to claims 14 and 17, wherein the confirmation information and the double check information also comprise a postal code of the client, wherein the authentication computer is arranged to check in a fourth checking step whether the postal code stored in the supplier information, the reply information, the confirmation information and the double check information is always the same.

19. A system according to any one of claims 13 – 18, characterized in that authentication information comprises a description of the products and/or services required by the client (K).

20. A system according to any one of claims 13 – 19, characterized in that the authentication unit (B) is arranged to store for a limited period of time the reply information and/or supplier information received from a client (K) and/or supplier (V).

21. A system according to at least claim 13, wherein the authentication computer forms part of a computer system of the supplier.

22. A system according to any one of claims 13 – 21, wherein the authentication computer is arranged to send the authentication information and receive the reply information in the form of a WAP or SMS message.

23. A data carrier, such as a CD-ROM, a smart card, a floppy disk, or the like, wherein the data carrier is provided with digital information, which, when entered into the computer of a client, makes this computer suitable as client computer apparently intended for a system according to any one of claims 13 – 22.

24. A data carrier according to claim 23, characterized in that it is a CD-ROM with credit card dimensions.

25. A data carrier according to claim 23 or 24, characterized in that the information stored thereon, when entered into a computer, is such that the client computer fully automatically leads the client through the order process.

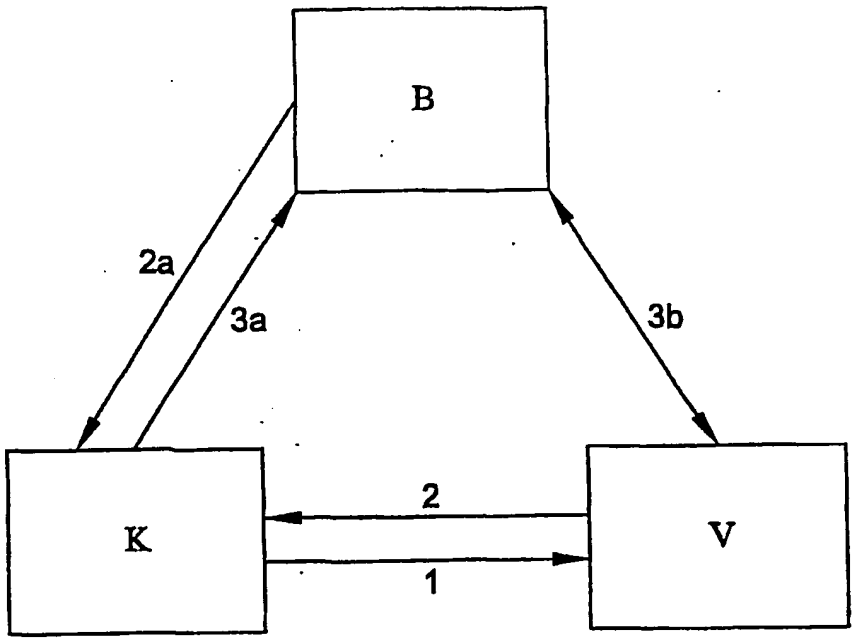


Fig. 1

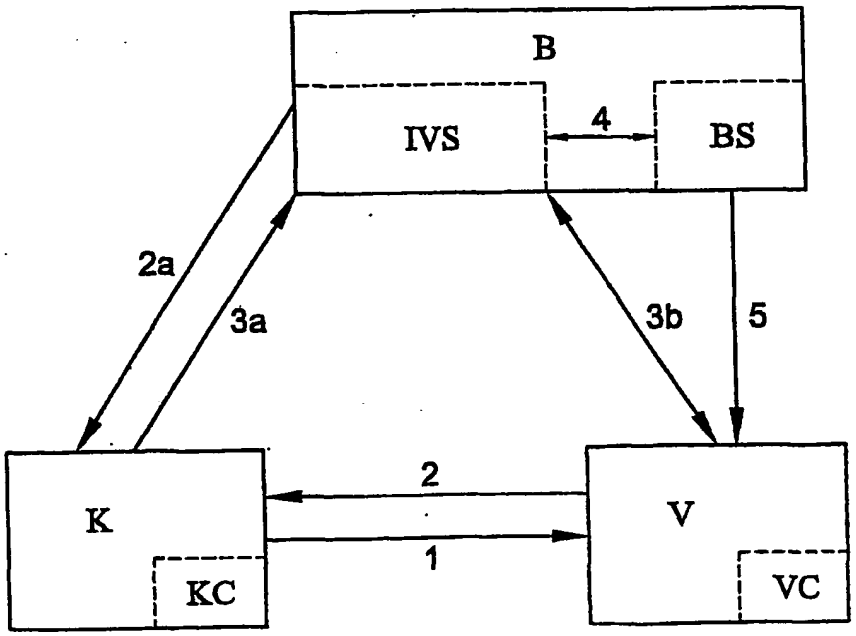


Fig. 2

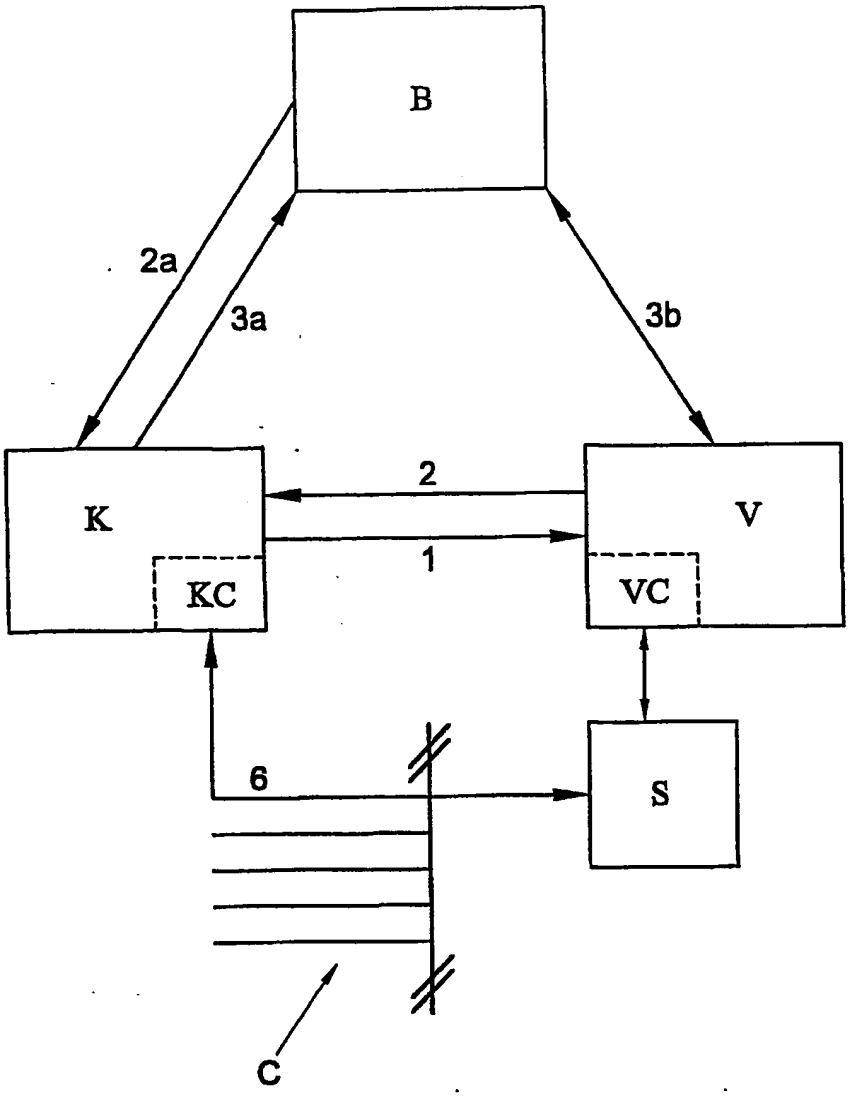


Fig. 3

INTERNAT' 'NAL SEARCH REPORT

Inte ial Application No
PC1/NL 01/00508

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60 G07F7/10 H04L12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 926 611 A (AT & T CORP) 30 June 1999 (1999-06-30) abstract; claims 1-7 column 6, line 12 - line 25 column 4, line 10 - line 28	1-25
X	EP 0 813 325 A (AT & T CORP) 17 December 1997 (1997-12-17) abstract; claims 11,31 column 1, line 45 -column 2, line 15	1-25
A	EP 0 765 068 A (AT & T CORP) 26 March 1997 (1997-03-26) abstract figure 1	1

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 September 2001	04/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Suendermann, R

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SIRBU M ET AL: "NETBILL: AN INTERNET COMMERCE SYSTEM OPTIMIZED FOR NETWORK-DELIVERED SERVICES" IEEE PERSONAL COMMUNICATIONS,IEEE COMMUNICATIONS SOCIETY,US, vol. 2, no. 4, 1 August 1995 (1995-08-01), pages 34-39, XP000517588 ISSN: 1070-9916 page 34 -page 39	1
A	WO 97 01920 A (IMMONEN PEKKA ;FINLAND TELECOM OY (FI)) 16 January 1997 (1997-01-16) abstract; claims 1-6	1

INTER TIONAL SEARCH REPORT
Information on patent family members

Int al Application No
PCT/NL 01/00508

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0926611 A	30-06-1999	EP 0926611 A2	30-06-1999
EP 0813325 A	17-12-1997	US 5778173 A	07-07-1998
		CA 2205124 A1	12-12-1997
		EP 0813325 A2	17-12-1997
		JP 10149397 A	02-06-1998
EP 0765068 A	26-03-1997	US 5745556 A	28-04-1998
		AU 709790 B2	09-09-1999
		AU 6571896 A	27-03-1997
		CA 2182818 A1	23-03-1997
		EP 0765068 A2	26-03-1997
		JP 9153964 A	10-06-1997
		US 5864610 A	26-01-1999
WO 9701920 A	16-01-1997	FI 953208 A	29-12-1996
		EP 0872117 A1	21-10-1998
		WO 9701920 A1	16-01-1997

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/003285 A1

(51) International Patent Classification[7]: G06F 17/60, G07F 7/10, H04L 12/14

(21) International Application Number: PCT/NL01/00508

(22) International Filing Date: 5 July 2001 (05.07.2001)

(25) Filing Language: Dutch

(26) Publication Language: English

(30) Priority Data:
1015612 5 July 2000 (05.07.2000) NL

(71) Applicant *(for all designated States except US)*: **HELCO AUTHENTICATION SERVICES B.V.** [NL/NL]; Schakelstede 1, NL-3431 HB Nieuwegein (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **JANSEN, Alexander, Theodorus** [NL/NL]; Mgr. Nolensstraat 10, NL-5431 WK Cuyk (NL).

(74) Agent: **PRINS, A. W.**; Vereenigde, Nieuwe Parklaan 97, NL-2587 BN The Hague (NL).

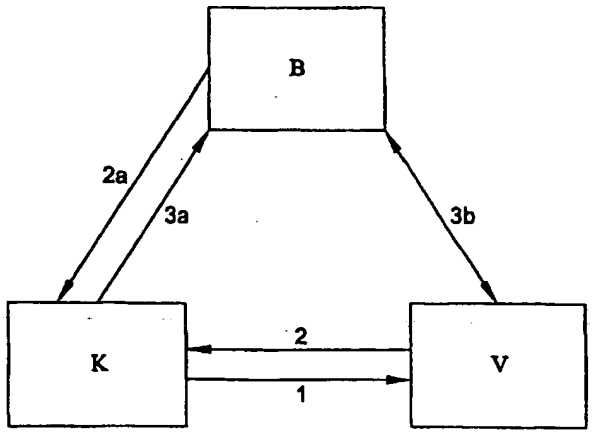
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SYSTEM AS WELL AS DATA CARRIER FOR AUTHENTICATING A CLIENT WHO DESIRES TO OBTAIN A SERVICE OR PRODUCT FROM A SUPPLIER



(57) Abstract: A method and a system as well as a data carrier for use in a system for authenticating a client who desires to obtain a service or product from a supplier, - wherein the client, via a first communication network, enters into communication with the supplier and gives order information, - wherein the supplier, on the basis of this order information, composes supplier information and gives it to an authentication unit, - wherein the authentication unit, on the basis of the supplier information received, composes authentication information and sends it to the mobile communication network number of the client, - wherein the client, with his mobile communication device, composes reply information and sends it to the authentication unit to confirm the authentication information received., - wherein the authentication unit performs at least one checking step, - wherein, if the or each checking step is followed by a confirmative reply, the authentication unit sends a supply release, - wherein, in a first checking step, the authentication unit checks whether the authentication information sent fits the reply information received.

WO 02/003285 A1

(48) **Date of publication of this corrected version:**
13 March 2003

(15) **Information about Correction:**
see PCT Gazette No. 11/2003 of 13 March 2003, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.